**IN THE CLAIMS:**

1. (Currently Amended) A method for managing public keys through a server, comprising:

receiving a client public key from a client at the server, wherein the client public key is produced by a client computer in response to user supplied information, and wherein the client public key is delivered as an email message;

storing the client public key in a database at the server, after confirming user identification;

allowing other clients to lookup the client public key in the database;

periodically sending a verification request from the server to the client asking if the client public key remains valid; and

if an affirmative response to the verification request is not received, removing the client public key from the database.

2. (Original) The method of claim 1, wherein storing the client public key in the database involves:

signing the client public key using a server private key; and

storing the signed client public key in the database.

3. (Original) The method of claim 1, further comprising:

receiving a request at the server to remove the client public key from the database;

if the request is signed with a corresponding client private key, removing the client public key from the database.

4. (Original) The method of claim 1, wherein the client public key is removed from the database only if an affirmative response is not received after sending multiple verification requests at different times.

5. (Original) The method of claim 1, wherein storing the client public key in the database at the server involves:

attempting to validate an association between a client email address and the client public key; and

if the association is successfully validated, storing the association in the database.

6. (Original) The method of claim 5, wherein the database contains at most one key for each email address.

7. (Original) The method of claim 5, wherein the database contains at most one email address for each key.

8. (Currently Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for managing public keys through a server, the method comprising:

receiving a client public key from a client at the server, wherein the client public key is produced by a client computer in response to user supplied information, and wherein the client public key is delivered as an email message;

storing the client public key in a database at the server, after confirming user identification;

allowing other clients to lookup the client public key in the database;

periodically sending a verification request from the server to the client asking if the client public key remains valid; and

if an affirmative response to the verification request is not received, removing the client public key from the database.

9. (Original) The computer-readable storage medium of claim 8, wherein storing the client public key in the database involves:

signing the client public key using a server private key; and

storing the signed client public key in the database.

10. (Original) The computer-readable storage medium of claim 8, wherein the method further comprises:

receiving a request at the server to remove the client public key from the database;

if the request is signed with a corresponding client private key, removing the client public key from the database.

11. (Original) The computer-readable storage medium of claim 8, wherein the client public key is removed from the database only if an affirmative response is not received after sending multiple verification requests at different times.

12. (Original) The computer-readable storage medium of claim 8, wherein storing the client public key in the database at the server involves:

attempting to validate an association between a client email address and the client public key; and

if the association is successfully validated, storing the association in the database.

13. (Original) The computer-readable storage medium of claim 12, wherein the database contains at most one key for each email address.

14. (Original) The computer-readable storage medium of claim 12, wherein the database contains at most one email address for each key.

15. (Currently Amended) An apparatus that facilitates managing public keys through a server, comprising:

a storing mechanism that is configured to store a client public key in a database at the server, after confirming user identification, wherein the client public key is produced by a client computer in response to user supplied information, and wherein the client public key is delivered as an email message;

a lookup mechanism that is configured to allow other clients to lookup the client public key in the database; and

a key removal mechanism that is configured to,

send a verification request from the server to the client asking if the client public key remains valid, and to

remove the client public key from the database, if an affirmative response to the verification request is not received.

16. (Original) The apparatus of claim 15, wherein the storing mechanism is configured to:

sign the client public key using a server private key; and to

store the signed client public key in the database.

17. (Original) The apparatus of claim 15, wherein the key removal mechanism is additionally configured to:

receive a request to remove the client public key from the database; and to

remove the client public key from the database if the request is signed with a corresponding client private key.

18. (Original) The apparatus of claim 15, wherein the key removal mechanism is configured to remove the client public key from the database only if an affirmative response is not received after sending multiple verification requests to the client at different times.

19. (Currently Amended) The apparatus of claim 15, wherein the storing mechanism is configured to:

attempt to validate an association between a client email address and the client public key; and to

~~storing~~ store the association in the database, if the association is successfully validated.

20. (Original) The apparatus of claim 19, wherein the database contains at most one key for each email address.

21. (Original) The apparatus of claim 19, wherein the database contains at most one email address for each key.